



CONTROLLI SUL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI - ART. 13 GDPR

Gent.le dipendente/collaboratore della Azienda Ospedaliero-Universitaria di Modena, con questo documento ti informiamo sui controlli che l'Azienda/datore di lavoro effettua sugli strumenti informatici utilizzati per fini lavorativi (posta elettronica, internet, telefonia).

Attività di controllo - principi generali

Le attività di controllo e vigilanza sugli strumenti informatici da parte della Azienda sono fondate sul principio della "proporzionalità" che si concretizza nella pertinenza e non eccedenza del controllo stesso; pertanto, i mezzi e l'ampiezza del controllo sono proporzionati allo scopo di proteggere i dati aziendali critici da accessi non autorizzati, abusi o violazioni, monitorando le attività al fine di individuare comportamenti anomali, prevenire minacce interne ed esterne, migliorare la gestione degli incidenti di sicurezza, pur nel rispetto della legittima aspettativa di riservatezza di dipendenti e collaboratori.

L'Azienda garantisce che i dati informatizzati da essa gestiti, nonché i sistemi di elaborazione dati e gli strumenti di telecomunicazione non saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114 Codice Privacy; artt. 4 e 8, L. 20 maggio 1970, n.300 – Statuto dei Lavoratori), se non nei limiti consentiti dallo Statuto dei Lavoratori, così come modificato dal D. Lgs. 151/2015 [Jobs Act] e dal Codice Privacy.

In ragione di ciò, l'Azienda non effettua verifiche, quali:

- Lettura e registrazione sistematica dei messaggi di posta elettronica o dei relativi dati esteriori, fatto salvo quanto tecnicamente necessario per svolgere il servizio e-mail;
- Riproduzione o eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- Lettura o registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- Analisi occulta di eventuali computer o dispositivi portatili affidati in uso;

L'Azienda si riserva tuttavia il diritto di effettuare controlli – meglio indicati in seguito - tesi a garantire il corretto utilizzo delle attrezzature informatiche aziendali e il corretto funzionamento del sistema informatico e di telefonia, in particolare nel caso in cui sospetti manomissioni alle configurazioni del sistema informatico, telematico, telefonico aziendale e/o accessi indebiti allo stesso, ovvero riscontri diffusioni indebite di informazioni atte a pregiudicare la sicurezza del sistema stesso o il suo buon funzionamento e/o a garantire ad altri accessi o privilegi non dovuti, o ancora abbia concrete ragioni che facciano ritenere che la sicurezza del sistema tecnologico aziendale sia minacciata.

Posta Elettronica

Il contenuto dei messaggi di posta elettronica, come pure i dati esteriori delle comunicazioni e i file allegati, riguarda forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali.

Tuttavia, quando motivi di sicurezza o di manutenzione lo richiedano, l'Azienda, previo avviso agli utenti interessati, può accedere alla configurazione delle caselle di posta elettronica per esclusive finalità tecniche. L'accesso alla configurazione di posta non comporta la visualizzazione dei messaggi della casella, salvo il caso eccezionale in cui il problema di sicurezza o di manutenzione non possa essere diversamente risolto. In quest'ultimo caso, l'utilizzatore interessato sarà informato prima dell'accesso. Inoltre, l'attività effettivamente eseguita sulle configurazioni (o sui messaggi di posta in caso eccezionale) viene sempre comunicata all'utente interessato al termine dell'intervento.

L'Azienda non conserva alcun log relativo al contenuto delle e-mail inviate e ricevute dagli utenti con il servizio di posta elettronica aziendale. L'unico log generato dal sistema è di tipo diagnostico con la finalità di individuare eventuali problemi in invio e ricezione della posta, di consentire lo svolgimento delle attività di analisi del Servizio ICT e le attività di indagine da parte della Autorità Giudiziaria, in caso accertamento di reati commessi mediante accesso al traffico telematico, per cui i dati di log costituiscono un elemento conoscitivo indispensabile. Alcuni log sono inoltre sottoposti a vincoli tecnici di conservazione non negoziabili, da parte di provider esterni di servizi (es.: antispam), funzionali allo svolgimento dei servizi stessi.

La conservazione dei log di posta elettronica è limitata ad un massimo di 90 giorni solari.

Il sistema di posta elettronica tiene traccia di tutte le e-mail inviate e ricevute, conservando nei log:

- identificativo della stazione di lavoro che ha inviato il messaggio
- data e ora
- indirizzo di posta del mittente
- indirizzo del destinatario
- oggetto

Questo log non è oggetto di operazioni di backup.

Internet

Tutti gli accessi a Internet vengono memorizzati in appositi file di log per finalità di sicurezza, di monitoraggio sul corretto funzionamento del sistema, di effettuazione di indagini statistiche. I log non sono accessibili per la consultazione, non sono oggetto di operazioni di backup e tengono traccia dei seguenti dati per ogni accesso:

- data e ora dell'accesso
- riferimento al sito visitato (URL)
- esito della consultazione
- tipologia di operazione richiesta e informazioni sugli eventuali file scaricati
- numero di byte trasferiti dall'elaboratore remoto e viceversa

La conservazione dei log di navigazione è limitata a un massimo di 90 giorni solari.

Qualora si rilevino le seguenti anomalie:

- traffico superiore del 20% rispetto alla media dell'ultimo semestre;
- utilizzo di porte e/o protocolli non utilizzati dai programmi aziendali;
- contemporanea presenza di sessioni parallele dirette al medesimo sito remoto;
- traffico dati diretto a siti presenti nella black-list
- altro incidente di sicurezza connesso con la navigazione in internet

L'Azienda emetterà un avviso generalizzato che informa della sospensione - per un periodo limitato e indicato nell'avviso stesso - dei controlli in forma anonima e del fatto che i log di sistema verranno utilizzati per l'individuazione delle cause. Durante questo periodo, in aggiunta alle informazioni enunciate in precedenza, verrà rilevato anche l'indirizzo IP di partenza della navigazione. Al termine del periodo di osservazione questi log saranno distrutti a cura del Servizio ICT.

I log potranno essere oggetto di provvedimenti da parte dell'Autorità Giudiziaria e in generale dei soggetti aventi funzioni ispettive e di controllo.

Telefonia

Per fini di controllo della spesa telefonica l'Azienda tiene traccia, attraverso i servizi del provider telefonico, delle telefonate effettuate, se queste costituiscono un onere economico per l'Azienda; mentre non sono tracciate le telefonate in ingresso. In particolare viene registrato:

- il numero del chiamante
- il numero chiamato
- data e ora di inizio e data e ora di fine della telefonata

La conservazione dei log di telefonia è limitata ad un massimo di 450 giorni solari.

Tale conservazione avviene in maniera disaggregata per poter confrontare gli andamenti di costo con i dati aggregati degli anni precedenti; qualora i dati evidenzino anomalie tali da giustificare controlli aggiuntivi, potranno essere ulteriormente approfonditi secondo una gradualità nei controlli che preveda prima il controllo del dato aggregato e la notifica di eventuali anomalie e solo successivamente, qualora il problema persista, un controllo sui dati disaggregati. Qualora l'integrità del sistema tecnologico dell'Azienda o la gravità del fatto lo rendano necessario sarà possibile accedere immediatamente al dato disaggregato; qualora possibile, gli approfondimenti sui dati che si rendessero necessari saranno condotti con verifiche a campione.

Modalità di conservazione dei dati

Tutti i log oggetto di conservazione sopra individuati sono conservati e protetti nel rispetto di misure di sicurezza adeguate e sono distrutti a cura del Servizio ICT alla scadenza del periodo di conservazione.

Esercizio dei diritti

In qualsiasi momento ciascun dipendente/collaboratore può esercitare il diritto di richiedere l'accesso ai propri dati personali, la rettifica di dati inesatti, l'integrazione di dati incompleti. Inoltre, nelle ipotesi e per i motivi stabiliti dalla legge, può richiedere la limitazione del trattamento dei suoi dati e può esercitare il diritto di opposizione al trattamento. A tal fine apposita istanza dovrà essere presentata alla Azienda contattando il Responsabile della protezione dati, contattabile all'indirizzo: dpo@aou.mo.it.

Ricorrendone i presupposti, ciascun dipendente/collaboratore ha altresì il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali, secondo le procedure previste.

Il Titolare del trattamento è l'Azienda Ospedaliero-Universitaria di Modena, con sede in Modena, via del Pozzo, 71